Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 2 | Issue : 4 | April 2016

DYNAMIC NETWORK SECURITY PROTECTION ON CLOUD COMPUTING

Akila J [1] | Vetripriya M [1] | Brigetta A [1] | Magesh Kumar k [1]

PG Scholar, Saveetha Engineering College Chennai, Tamilnadu.

ABSTRACT

This paper focuses on DDoS problem and trying to give solution using auto correlation and alert generation methods. Cloud trace back model has efficient and it's dealing with DDoS attacks using back propagation neural network method and finds that the model is useful in tackling Distributed Denial of Service attacks. Distributed denial of service attacks has become more sophisticated as to exploit application-layer vulnerabilities. NICE (Network Intrusion Detection and Countermeasure Selection) is used to propose multiphase distributed vulnerability detection for attack measurement, and the countermeasure selection mechanism which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. The systems and security evaluations demonstrate the efficiency and effectiveness of the solution.

KEYWORDS: cloud computing, DDoS attack, intrusion detection, protection, security.

I. INTRODUCTION

Cloud Computing is a catchword in today's IT industry. Cloud computing uses modern web and virtualization to dynamically provide various kinds of electronic provisioned services include some common features such as scalability, pay-as-you-go, on-demand, self- configuration, and self-maintenance and Software as a Service (SaaS). The clouds consider security as the most important factor. A recent Cloud security Alliance (CSA) survey shows that all security abuse, issues and nefarious use of cloud computing is considered as the top security threat. In traditional data centers, where system administrators have full control over the host machines, then vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known the security holes in cloud data centers, where cloud users usually have privilege to control software installed on their managed Vms (Virtual Machine), may not work effectively and can violate the service level agreement. In this project the challenges is to establish an effective vulnerability/attack and response system for accurately identifying attacks and minimizing the impact of security breaches to the cloud users. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the Identity privacy. Some flaws will be expected When membership revocation in the cloud. In multi-owner cloud, minimizing the complexity of key management becomes a very difficult one. Mona methods are complex it difficult to define all the features which were given by cloud admin.

The main concept is to solving a major security challenge on the Internet is the existence of the large number of compromised machines. Such machines have increasingly used to launch various security attacks, having spamming and spreading malware, DDoS, and identity theft. Identifying and cleaning compromised machines in a network remain a significant challenge for system administrators of networks of all sizes.

The detection of the compromised machines in a network that are used for sending unwanted messages has been focused, which are commonly referred to as spam zombies. The solutions are given for preventing our network from nefarious things. The experimental results show that the proposed technique is effective and can detect DDoS attacks with high detection rate.

II .RELATED WORKS

Cloud computing is still in its infancy, current adoption is associated with many challenges like security, availability, and performance. In cloud computing, where infrastructure is shared by potentially millions of users, DDOS attacks have greater impact than against single tenanted architecture. This paper tested the efficiency of a cloud trace back model in dealing with DDOS attacks using back propagation neural network and finds that the Model is useful in tackling distributed denial of service attacks Compromised machines are one of the key security threats on the Internet; they are often used to launch various security attacks such as spamming, spreading malware, DDoS, and identity theft. Spamming provides a key economic incentive for attackers to recruit the largest number of compromised machines. Thus the detection of the compromised machines is focused in networks that are involved in the spamming activities, commonly known as spam zombies. An effective spam zombie detection system has been developed and named as SPOT by monitoring outgoing messages of a network. SPOT is designed on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded as false positive and false negative error rates. They also compare the performance of SPOT with two other spam zombie detection algorithms based on the number and percentage of spam messages originated or forwarded by internal machines, and show that SPOT out perform these two detection algorithms.

Intrusion Detection Systems (IDS) are widely deployed in computer networks. As modern attacks are more sophisticated and the number of sensors and network node grows, the problem of false positives and alert analysis becomes more difficult to solve. For representing the environment information as well as potential exploits, this existing vulnerability and their Attack Graph are used. It is useful for networks to generate an AG and to organize certain vulnerabilities in a reasonable way. In this work, thus the correlation algorithm is designed and based on AGs that is capable of detecting multiple attack scenarios for forensic analysis. To adjust the robustness and accuracy. A formal model of algorithms is presented and an implementation is tested to analyze the different parameters on a real set of alerts from a local network.

In this work an automated technique is used for generating and analyzing attack graphs. The technique is based on symbolic model checking algorithms, let us construct attack graphs automatically and efficiently guard against. They implemented our technique in a tool suite and tested it on a small network example, which include models of a firewall and an intrusion detection system. A novel AT paradigm is used call attack countermeasure tree (ACT) whose structure takes into account attacks as well as counter measures (in the form of detection and mitigation events).

By using the greedy and branch and bound techniques to study several objective functions with goals such as minimizing the number of countermeasures, security cost in the ACT and maximizing the benefit from implementing a certain countermeasure set in the ACT under different constraints. Casting each optimization problem into an integer programming problem which also allows us to find optimal solution even in the absence of probability assignments to the model. Our method scale well, for large ACTs and it is efficient with other approaches. This paper proposed a model to probability metrics based on attack graphs as a special Bayesian Network. This approach provides a theoretical foundation to such metrics. It can also give the capabilities of using conditional probabilities to address the general cases of interdependency between vulnerabilities.

III.PROPOSED WORK

In this paper, it proposed the NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures introduced a “soft-control” scheme for the attack response based on the underlying state process. The schemes reshape the suspicious sequences according to the profile of normal behavior that is converting the suspicious sequence into a relatively normal one by partly discarding its most likely malicious requests instead of denying the entire sequences. The proposed scheme is based on network behavior analysis. It maps Open Flow networking programming access behavior to a NICE model. In cloud system, DDoS attacks have been receiving more attention than the previous approaches. Here clients are evaluated by trust management mechanism and then the application layer DDoS is mitigated by giving priority to good users. Our work shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions.

Copyright© 2016, IERJ. This open-access article is published under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License which permits Share (copy and redistribute the material in any medium or format) and Adapt (remix, transform, and build upon the material) under the Attribution-NonCommercial terms.

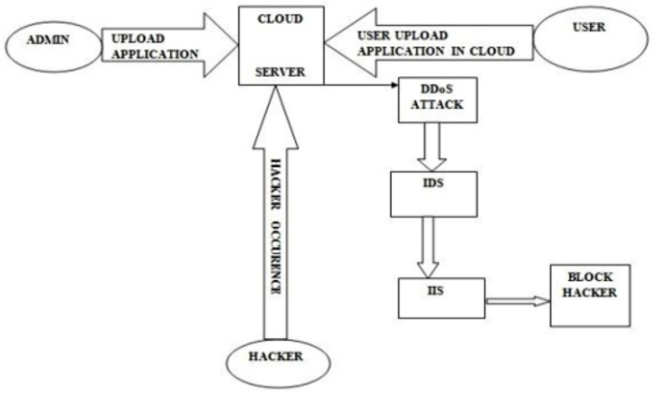


Fig 1: Architecture Diagram

1.a) Denial Attacks

There are many kinds of hackers on the Inter net, with a wide range of hacking skills which may have read of sophisticated criminal rings, phishing scams, etc. that are motivated for profit. If there is a victim of a Denial of Service attack, who is probably not a victim of one of these sophisticated criminal organizations. Generally, Denial of Service Attacks is an act of vandalism and the attacker instigating the attack has no financial motive. Although a DoS attack can be extremely damaging to the business/website, these types of attacks can be easily setup by an inexperienced hacker with limited technical ability.

In a denial-of-service (DoS) attack, an attacker attempts to prevent users from accessing information or services. By targeting our computer and its network connection, computers and network of the sites when a user is trying to use, an attacker may be able to prevent it from accessing email, websites, online banking accounts, etc., or other service that rely on the affected computer. The most common DoS attack occurs when an attacker cloud network with information. When you type a URL of a particular website, you are sending a request to site's computer server to view the page.

The server can process a certain number of requests at once, so if attackers overload the server with requests, it can't process the request. This is a denial of service because you can't access that site. An attacker can use spam email to launch a similar attack on your email account. If your mail account supplied by the employer or available through a free service such as Yahoo mail or Hot mail, you are assigned a specific quota, it limits the amount of data you can have in your account at any given time. By sending large email messages to the account, an attacker may consume your quota; prevent you from receiving legitimate messages.

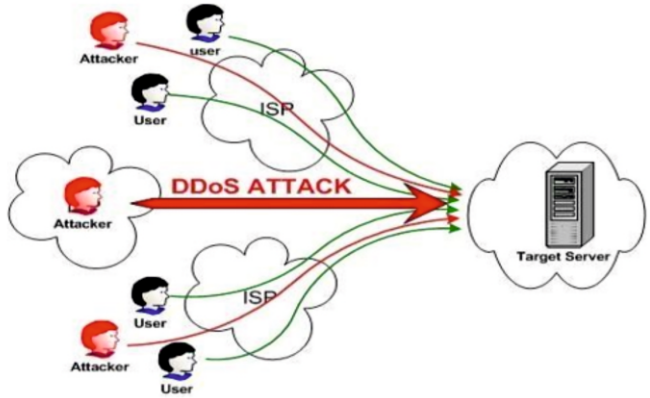


Fig 2: DDoS Attack

1.b) Detecting a Denial of Service

A distributed denial of service attack tells all coordinated systems to send a stream of requests to a specific server at the same time. This request may be a simple ping or a more complex series of packets. If the server cannot respond to a large number of simultaneous requests, incoming request will become queued. This backlog of requests can result in a slow response time or a no response at all. When this server is unable to respond to requests, the DoS attack has succeeded. DoS attacks are a common method hackers use to attack websites. Since flooding a server with requests, it does not require any authentication; even a highly secured server is vulnerable. A single system is typically not capable of carrying out a successful DoS attack. Therefore, a hacker can create a botnet to control multiple computers at once.

A botnet may be used to carry out a DDoS attack, which is more effective than an attack from a single computer. Denial of service attacks can be difficult, especially when They cause large websites to be unavailable during high- traffic times. Fortunately, software has been developed to detect DoS attacks and limit their effectiveness. While many well-known websites, like Twitter, Google, and Word Press, have all been targets of Dos attacks in the past, they have been able to improve their security systems and prevent further service interruptions.

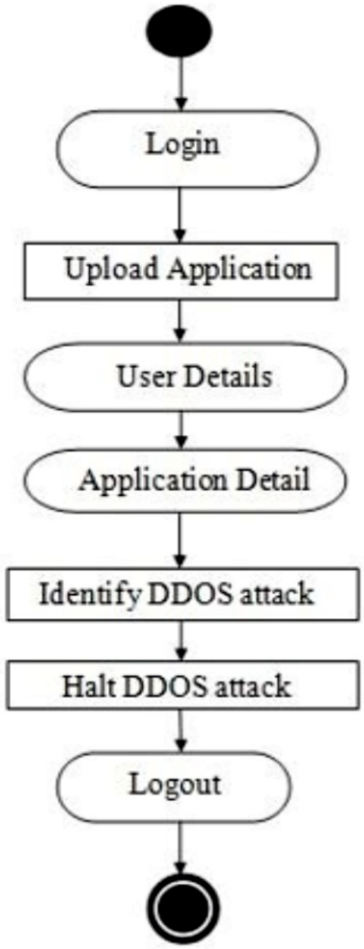


Fig 3: Activity Diagram

IV IMPLEMENTATION

This method will quickly mitigate the attack, but it will not stop completely. First step it can't block the attack at the router as described above, but still they want to implement some of the steps below. This method will tell IIS (web server) to stop servicing requests from these hacked IP addresses. However, these hacked machines will be able to open (unused) network connections to your machine.

Still now they can see these connections using net stat; though many connections which are not "ESTABLISHED", but the attacker has to use many more machines to attack any site in order to cause a Denial of Service, so this method may work well for us in the short run. But modern DDoS attacks are getting insanely quiet and large often can be much bigger than the finances will allow in terms of bandwidth. Plus, sometimes if it's not on our website that will be targeted, a fact of many administrators tends to forget.

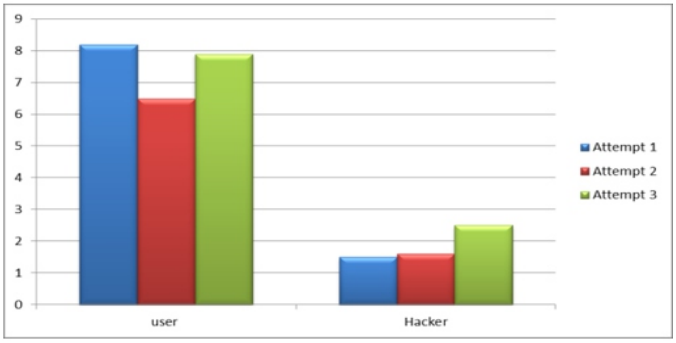
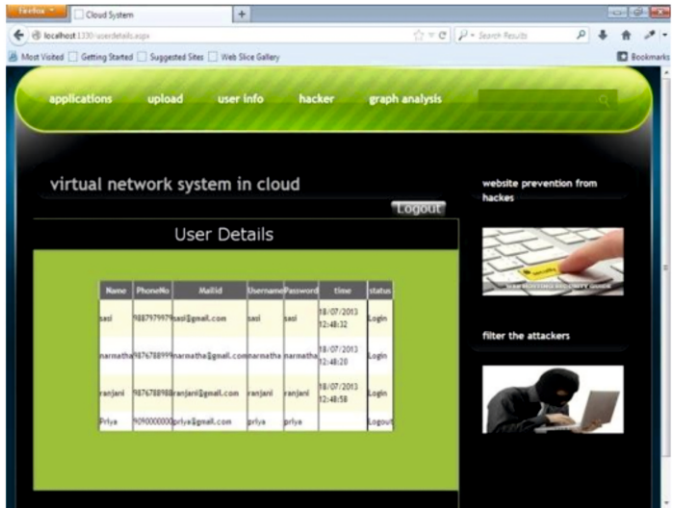
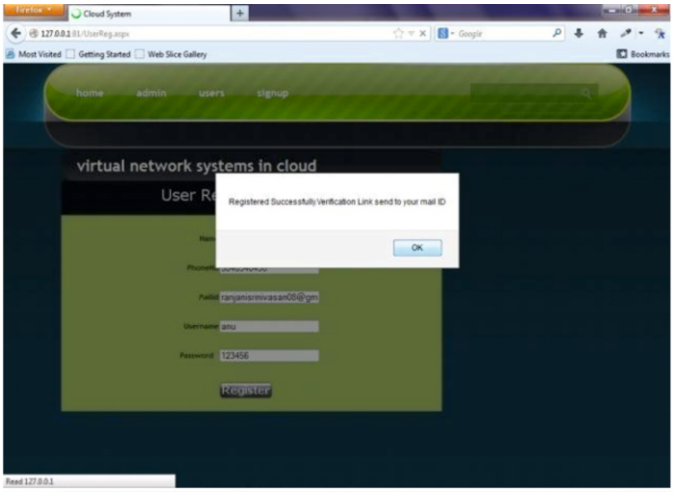
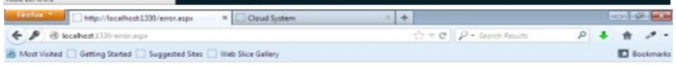


Fig 4: Performance of Attempts



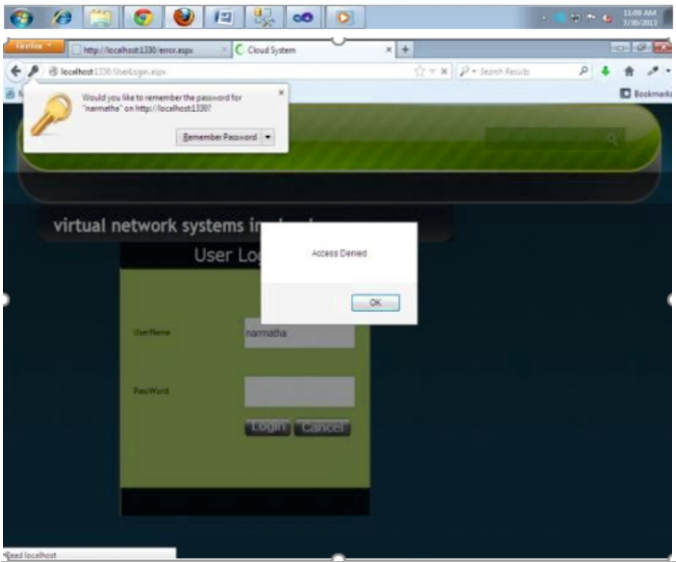




Service Unavailable

HTTP Error 503:

The Service Is Unavailable



V. RESULT AND DISCUSSIONS

DoS attacks are a common method hackers use to attack websites. Flooding a server with requests does not require any authentication; even a more highly secured server is vulnerable. But however, a single system is typically not capable of carrying out a successful DoS attack. Therefore, a hacker can create a botnet to control multiple computers at once. A bonnet may be used to carry out a DDoS attack, which is more effective than an attack from a single computer. Denial of service attacks can be problematic, especially when they cause large websites to be unavailable during high-traffic times. Fortunately, the security software has been developed to detect DoS attacks and limit their effectiveness. While many well-known websites, like Twitter, Google, and Word Press, have all been targets of denial of service (DoS) attacks in the past, they have been able to improve their security systems and prevent further service interruptions.

VI. CONCULSION

In dynamic security protection on cloud computing is used to filter the attack traffic from the aggregated proxy-to- server traffic, it is a new problem for the DDoS detection. Our experiment confirmed the effectiveness and robustness of the proposed scheme. By using the method developed an effective spam zombie detection system named NICE by monitoring outgoing messages in a network.

VII. REFERENCES

1. B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. And Informatics (ICCCI'12), Jan. 2012.
2. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr.2012.
3. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.
4. S. Roschke, F. Cheng, and C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph," Proc. Fourth Int'l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.
5. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), June2012.
6. M. Frigault and L. Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs," Proc. IEEE 32nd Ann. Int'l Conf. Computer Software and Applications (COMPSAC '08), pp. 698-703, Aug. 2008.
7. P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph based network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS'02), pp. 217-224, 2002.
8. X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic-Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005.
9. R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Framework and Techniques," Proc. ACM Int'l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06), pp.37:1-37:10, 2006.
10. L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts," Computer Comm., vol. 29, no. 15, pp.2917-2933, Sept. 2006.
11. N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb. 2012.
12. Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks," ONF White Paper, Apr. 2012.
13. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J.Turner, "OpenFlow: Enabling Innovation in Campus Networks," SIGCOMM Computer Comm. Rev., vol. 38, no. 2, pp. 69-74, Mar. 2008.
14. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," ACM Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.
15. H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec.2010.